Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 376-379, April-June 2018

Advanced Security Systems Using Wireless Technology

Dr.B.Paulchamy[1], R.Punitha[2], B.Navin Kumar [3], P.Prasanth[4], M.Prithiviraj[5] and S.M.Sanmathi[6]

[1]Professor & Head, [2]Assistant Professor, [3,4,5,6]UG Students, Hindusthan Institute of Technology, Coimbatore, Tamilnadu, India.

Article Received: 29 January 2018 *Article Accepted: 26 February 2018* *Article Published: 17 April 2018*

ABSTRACT

According to the novel taxonomy of IOT vision, a case study of military live simulation will be presented to highlight components and interactions of the systemic and cognitive approach. Then, a discussion of security questions about privacy, trust, identification and access control will be provided, and different research challenges will be highlighted. According to the novel taxonomy of IOT vision, a case study of military live simulation will be presented to highlight components and interactions of the systemic and cognitive approach. Then, a discussion of security questions about privacy, trust, identification and access control will be provide, and different research challenges will be highlighted. In this paper we are introducing the idea of live simulation, metal detection, attacking and self-destructing robot which can be used as an application in border security. The objective of this paper is to reduce manpower in highly risky areas by replacing manpower by these robots which prevent the loss of human loss.

Keywords: IOT, security, metal sensor, vibration sensor, gun, PIC, self-destruction.

1. INTRODUCTION

Some analysts assert that they symbolize a transformation in warfare, similar in scale to the gunpowder revolution. Some even hypothesize that robot might one day replace manned aircraft in combat and logistics roles. However, these projections are likely to prove unrealistic, given the fundamental limitations of robots. Such limitations are not just technological, but also doctrinal. Two key questions arise while assessing the military impact of robots. First, do they represent an evolution or a revolution in military technology. The former implies a gradual change in operating systems and practices, which can be countered through matching innovations. The latter implies that robots convey an asymmetric and possibly decisive advantage to the side that possesses them. A long-term historical perspective would suggest that drones are evolutionary, not revolutionary.

2. BLOCK DIAGRAM

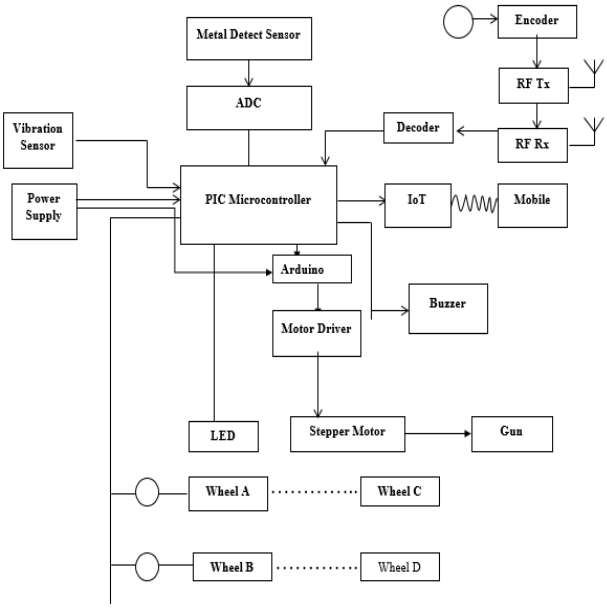

Fig 1: Block Diagram

PIC 16F877A is used to encode and decode RF signals. The motor drive is driven according to the commands given in the RF signals which are encoded and decoded by PIC16F877A controller. The vibration sensor and the metal detectors re controlled by the instructions fed by the controller. Live streaming is done using IOT. All the programs are fed to the controller through MP lab and the simulation is done with the help of Proteus8.

3. PROPOSED SYSTEM

Now-a-days, Automated systems have less manual operations, flexibility, reliability and accuracy. Here, the robot designed is also used to detect bomb and attack the unwanted person (related weapon) by sending the robot to the respective place. A person can operate the system from personal computer through wireless RF control. The Wireless IR camera is be operated remotely for monitoring as well as controlling purpose. In the dark nights or dark places, this robot is capable of capturing videos, and then transmitting them remotely to a PC or TV by using WI-FI technology. In order to reduce the human losses. Motors are fitted to the robot. A micro controller is used to control all operations. According to the motor operations the robot will operate as specified in the program, whenever any obstacle is detected. Highly alert for people. Monitoring easy through Computer. Detecting persons through wireless IR camera. Attacking unrelated person to current situation by using gun. Password or some advanced method based access system.

4. PROJECT SUMMARY

To reduce human effort and death in war by replacing manpower with robots to provide border security by continuous surveillance and counter-attack can be all done in a single invention. Here, in this project the robot designed can be replaced instead of manpower but is operated manually by human in the control area. Live simulation is done by using IOT through IR camera. Counter-attack and attacking of any unauthorized entry is done through the armed weapon fixed in the robot which is instructed by the control person in the control area. Land mines are also detected using metal detectors.

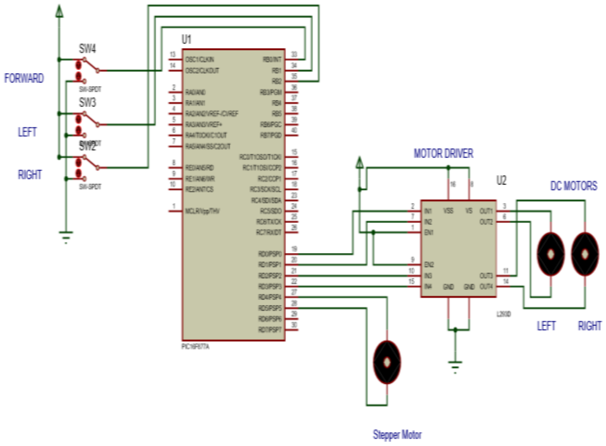

Fig 2: Software simulation-PIC 16f877a

Another important addition to the robot is self-destruction mode which will be activated when the robot is tried to be destroyed by any means the robot will be automatically self-destroyed. All the controls are transmitted and received through RF signals. By introducing these robots for surveillance in border security loss of manpower can be drastically reduced mean while all the controls of the robot are not automated since fully automated robots can be a threat to the people of its own country, but here these robots are operated by the instructions given manually by the authorized who is under 24x7 surveillance through live streaming.

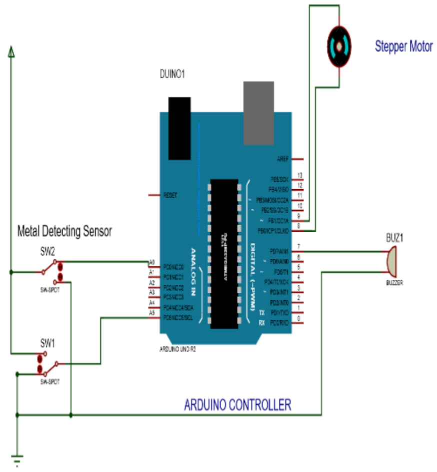

Fig 3: Software simulation –arduino

5. ADVANTAGES

An affordable Technology with high end advantage. Can help tracking alive human beings. View the status of the person alive. The place can be monitored remotely by moving the robot. The video streaming can be made much faster using Advanced Multimedia API.

6. APPLICATION

Robot finds its application in Aerial Photography. Can be implemented for search and rescue operations. In the field of agriculture. Robot for shipping and delivery. Robot for Safety Surveillance

7. CONCLUSIONS

Recent advances in IOT technology, as reviewed in this article, stand to both greatly change and benefit existing military operations. In part, these benefits are expected to emerge from combined use of Commercial off the Shelf (COTS) devices and specialized middleware solutions. However, co-deployment and coexistence of commercial IOT and military systems raise many challenges. A common theme for these challenges lies in management of limited computational and networking resources, as compared to existing commercial services. We discussed the relationship of these research challenges to military contexts and provide a discussion of how middleware solutions, like ACM and SPF, aim to address many of these challenges through novel methods of development and deployment for cyber-physical applications and of information prioritization. The proliferation of IOT-generated information will occur in sufficient volume to mandate a need for architectures and frameworks that filter, prioritize, and intelligently deliver intent driven and context sensitive decision support. We illustrate that middleware solutions can provide capabilities that mitigate some of the negative effects of IOT-enabled military applications; particularly those that operate in tactical environments. We expect that in the near future, middleware solutions such as SPF will become increasing information oriented – converging on greater use of technologies such as Value of Information and semantically-enabled content that is enriched with trust and provenance metadata.

REFERENCES

[1] H. Zhang and S. Li, “Internet of things and its influence on army informationization construction,” Journal of Military Communications Science, vol. 1, pp. 81-82, 2010.

[2] C. Amardeo and J. G. Sarma, “Identities in the future IOT,” Wireless Pers. Commun., vol. 49, pp. 353-363, 2009.

[3] W. Gong and M. Sun, “Military IOT-To perceive modern military logistics,” Military Logistics and Purchasing, vol. 6, pp. 68-71, 2009.

[4] H. Wang, J. Shen, Y. Shi, “New trends in the development of supply chain management based on IOT,” Commercial Times, vol.3, pp. 86-87, 2009.

[5] Y. Hu, Y. Liu, and H. Zang, “The design of vehicle emergent calling system based on GPRS,” 2007 IEEE International Conference on Automation and Logistics, Jinan, China, pp. 1220-1224, 2007.

[6] Y. Peng, “Application of internet of things technology in ammunition container road transport,” National defense traffic engineering and technology, vol.4, pp. 7-9, 2014.

[7] O. Vermesan et al, “Internet of things strategic research roadmap,” EPoSS. Sep 2009.

[8] A.Al-Fuqaha, M.Guizani, M.Mohammadi, M.Aledhari, M.Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Communications Surveys & Tutorials, Vol. 17, No. 4, pp. 2347-2376, Fourth quarter 2015.